## CLAIMS

1. A cryptography acceleration chip, comprising:

a plurality of cryptography processing engines; and

a packet distributor unit configured to receive data packets and matching classification information for the packets, and to input each of the packets to one of the plurality of cryptography processing engines;

wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a given packet flow in parallel while maintaining per flow packet order.

2. The chip of claim 1, wherein said distributor unit processes received packet and matching classification information sequentially.

3. The chip of claim 1, wherein said plurality of cryptography engines process the input packets in parallel.

4. The chip of claim 1, wherein said distributor unit inputs packets to the cryptography engines in round-robin fashion.

5. The chip of claim 4, wherein said distributor unit reads packets output from the cryptography engines in the same round-robin fashion.

6. The chip of claim 1, wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a plurality of packet flows in parallel while maintaining packet ordering across the plurality of flows.

7. The chip of claim 1, wherein said packets require IPSec cryptography processing.

8. The chip of claim 7, wherein said chip operates at sustained rate of at least one Gigabit/s in full duplex mode.

9. The chip of claim 1, wherein said distributor unit further comprises an order maintenance retirement unit configured to enable the plurality of cryptography engines to process incoming packets in out-of-order fashion.

10. The chip of claim 9, wherein said order maintenance retirement unit extracts processed packets from a retirement buffer and outputs them from the chip in the same order in which they were received by the chip.

11. A method for accelerating cryptography processing of data packets, the method comprising:

receiving a plurality of data packets on a cryptography acceleration chip;

processing the data packets and matching classification information for the packets;

distributing the data packets to a plurality of cryptography processing engines for cryptographic processing;

cryptographically processing the data packets in parallel on the plurality of cryptography processing engines;

outputting the cryptographically processed data packets from the chip in correct per flow packet order.

12. The method of claim 11, wherein said processing of received packet and matching classification information is done sequentially.

13. The method of claim 11, wherein said cryptographic processing of said packets on said plurality of cryptography engines is done in parallel.

14. The method of claim 11, wherein said distribution of packets to the cryptography engines is done in round-robin fashion.

15. The method of claim 14, wherein said outputting of packets from the cryptography engines is done in the same round-robin fashion.

16. The method of claim 11, wherein the combination of said distribution and cryptographic processing further maintains packet ordering across a plurality of flows.

17. The method of claim 11, wherein said packets require IPSec cryptography processing.

18. The method of claim 17, wherein said chip operates at sustained rate of at least one Gigabit/s in full duplex mode.

19. The method of claim 19, further comprising managing the processing of the packet data through the plurality of cryptography processing engines without requiring any attached local memory.

20. An IPSec cryptography acceleration chip, comprising:

an external system bus interface unit;

a packet classifier unit;

a packet distributor unit;

a FIFO input buffer connected to the packet classifier unit;

a FIFO output buffer connected to packet distributor unit;

a plurality of cryptography processing engine units connected to the packet distributor unit; and

a control processor that manages the processing of packets through the chip.

22. The IPSec cryptography acceleration chip of Claim 21, further comprising:

a packet splitting unit, in which incoming packets are split into fixed-sized cells.

23. A network communication device, comprising:

a central processing unit;

a system memory;

a network interface unit;

a cryptography acceleration chip comprising:

a plurality of cryptography processing engines; and

a packet distributor unit configured to receive data packets and matching classification information for the packets, and to input each of the packets to one of the plurality of cryptography processing engines;

wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a given packet flow in parallel while maintaining per flow packet order.

an internal bus that connects the central processing unit, the system memory, the network interface unit, and the cryptography acceleration chip.

23

24. The device of claim 23, wherein the internal bus is a high speed switching matrix.